

October 1, 2020

Sent via email

Washington State Attorney General's Office
1125 Washington St SE
PO Box 40100
Olympia, WA 98504
security.breach@atg.wa.gov

re: Gallaudet University notification of Blackbaud data security event

Dear Attorney General,

Gallaudet University ("Gallaudet") was informed by Blackbaud, a third-party provider that Gallaudet uses to manage its donor databases, that information about Gallaudet's donors was involved in a data security incident that occurred during May 2020. Unfortunately, although Blackbaud's email was sent mid-July 2020, our privacy team did not receive the notification in time to take earlier action. We have since taken steps to ensure that any notifications we receive in the future will immediately be relayed to the correct personnel, which will trigger our data security protocol.

As part of our internal investigation, we reached out to Blackbaud to learn more about the incident and how it affected us. According to the information we received, the cybercriminal removed a backup copy that contained donor information from many other organizations, including Gallaudet. This backup copy was identified to contain the personal information of 1,195 Gallaudet constituents who are Washington residents.

The information in the backup copy contained donation information, including names of donors, contact information, and dates of birth. Blackbaud received confirmation that the copy of the backup file the cybercriminals obtained has been destroyed after Blackbaud paid the ransom. We have no evidence that these events have resulted in the misuse of personal information.

We began notifying Washington state residents via letter on October 2, 2020 and have included a sample copy of the letter.

If your office requires any further information in this matter, please contact us at privacy@gallaudet.edu.

Sincerely,

A handwritten signature in black ink, appearing to read "Jared Evans", with a stylized flourish at the end.

Jared Evans
Information Security Officer

<Name>
<Address>

September 25, 2020

Dear <NAME>,

Gallaudet University (“Gallaudet”) was recently notified about a data security incident. We are sending this letter to let you know that the incident may have involved personal information, collected when a donation is made to Gallaudet.

What happened:

We were notified that our donor database service provider, Blackbaud, Inc., discovered and stopped a ransomware attack that had occurred sometimes in May 2020. This was a security event that involved data from many other nonprofit organizations and other entities that relied upon Blackbaud to manage their donor information. According to Blackbaud, the cybercriminal removed a backup copy of donor information that Blackbaud maintained for us and which may have contained some of your personal information. Blackbaud paid a ransom demand and received confirmation from the cybercriminal that the backup copy obtained during the attack was destroyed. For more information about this data security event, Blackbaud released a public statement acknowledging this incident and describing its cybersecurity practices, located at www.blackbaud.com/securityincident.

What information was involved:

The affected file contained information about donations, including the names of donors, contact information and dates of birth. We have no evidence that personal information impacted by these events have been misused. However, we have included information about steps you can take to protect yourself.

What we are doing:

Data security is something we take seriously. Once we realized that the situation affected our constituents, we launched an internal investigation to understand how this happened, which included reaching out to Blackbaud. Blackbaud advised us that they have made several changes to ensure protection of personal information in the future, including improved access management, network segmentation, and deployment of additional endpoint monitoring.

What you can do:

While we do not have evidence to believe that any personal information has been misused, we encourage you to take precautions to protect yourself.

- Regularly review and monitor your account statements and credit history for any unauthorized transactions or activity and immediately report any such unauthorized activity you identify to your financial institutions.
- Be careful with emails that request sensitive information, such as passwords, social security numbers or bank account information, even if it appears to be sent from someone you know.

- If you suspect you are a victim of identity theft or fraud, you can file a report with the police or law enforcement.
- Contact the U.S. Federal Trade Commission (www.consumer.gov/idtheft) or your state attorney general to learn more about protecting yourself against identity theft.
- U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com.
- North Dakota residents may obtain information about preventing identity theft at <https://attorneygeneral.nd.gov/consumer-resources/identity-theft/reporting-identity-theft>.
- Washington residents may obtain information about preventing identity theft at www.atg.wa.gov/identity-theftprivacy.

For more information:

If you have questions or concerns that this letter does not answer, please email us at privacy@gallaudet.edu and we will respond to your email as soon as we can. Again, we regret any concern this matter may have caused.

Sincerely,

Nicholas Gould, '09
Executive Director of Institutional Advancement